

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-313

Vulnerability Summary for the Week of November 2, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- shockwave_player	Array index error in Adobe Shockwave Player before 11.5.2.602 allows remote attackers to execute arbitrary code via crafted Shockwave content on a web site. NOTE: some of these details are obtained from third party information.	2009-11-04	9.3	CVE-2009-3463 CONFIRM
adobe -- shockwave_player	Adobe Shockwave Player before 11.5.2.602 allows remote attackers to execute arbitrary code via crafted Shockwave content on a web site, related to an "invalid pointer vulnerability," a different issue than CVE-2009-3465. NOTE: some of these details are obtained from third party information.	2009-11-04	10.0	CVE-2009-3464 BID CONFIRM
adobe -- shockwave_player	Adobe Shockwave Player before 11.5.2.602 allows remote attackers to execute arbitrary code via crafted Shockwave content on a web site, related to an "invalid pointer vulnerability," a different issue than CVE-2009-3464. NOTE: some of these details are obtained from third party information.	2009-11-04	10.0	CVE-2009-3465 XF VUPEN BID CONFIRM SECTRACK
adobe -- shockwave_player	Adobe Shockwave Player before 11.5.2.602 allows remote attackers to execute arbitrary code via a crafted web page that triggers memory corruption, related to an "invalid string length vulnerability." NOTE: some of these details are obtained from third	2009-11-04	9.3	CVE-2009-3466 CONFIRM

	party information.			
blender -- blender	Blender 2.34, 2.35a, 2.40, and 2.49b allows remote attackers to execute arbitrary code via a .blend file that contains Python statements in the onLoad action of a ScriptLink SDNA.	2009-11-06	9.3	CVE-2009-3850 BID BUGTRAQ MISC
eeye -- retina_network_security_scanner	Buffer overflow in eEye Retina WiFi Scanner 1.0.8.68, as used in Retina Network Security Scanner 5.10.14, allows user-assisted remote attackers to cause a denial of service (application crash) or execute arbitrary code via a .rws file with a long RWS010 entry.	2009-11-04	9.3	CVE-2009-3859 EEYE
ibm -- ibm_runtimes_for_java_technology	Unspecified vulnerability in the XML component in IBM Runtimes for Java Technology 5.0.0 before SR10 has unknown impact and attack vectors, related to the "updated version of XML4J 4.4.17."	2009-11-03	7.5	CVE-2009-3852 XF VUPEN BID AIXAPAR SECUNIA
ibm -- lotus_notes_intellisync	Buffer overflow in the IBM Lotus Notes Intellisync ActiveX control in Inresobject.dll in BlackBerry Desktop Manager in Research In Motion (RIM) BlackBerry Desktop Software before 5.0.1 allows remote attackers to execute arbitrary code via a crafted web page. NOTE: some of these details are obtained from third party information.	2009-11-04	9.3	CVE-2009-0306 CONFIRM
ibm -- tivoli_storage_manager_client	Buffer overflow in the client acceptor daemon (CAD) scheduler in the client in IBM Tivoli Storage Manager (TSM) 5.3 before 5.3.6.7, 5.4 before 5.4.3, 5.5 before 5.5.2.2, and 6.1 before 6.1.0.2, and TSM Express 5.3.3.0 through 5.3.6.6, allows remote attackers to execute arbitrary code via unspecified vectors.	2009-11-04	9.3	CVE-2009-3853 CONFIRM
ibm -- tivoli_storage_manager_client	Buffer overflow in the traditional client scheduler in the client in IBM Tivoli Storage Manager (TSM) 5.3 before 5.3.6.7 and 5.4 before 5.4.2 allows remote attackers to execute arbitrary code via unspecified vectors.	2009-11-04	10.0	CVE-2009-3854 CONFIRM
ibm -- tivoli_storage_manager_client	Multiple unspecified vulnerabilities in the (1) UNIX and (2) Linux backup-archive clients, and the (3) OS/400 API client, in IBM Tivoli Storage Manager (TSM) 5.3 before 5.3.6.6, 5.4 before 5.4.2, and 5.5 before 5.5.1, when the MAILPROG option is enabled, allow attackers to read, modify, or delete arbitrary files via unknown vectors.	2009-11-04	9.3	CVE-2009-3855 CONFIRM
poppler -- poppler	Multiple integer overflows in Poppler 0.10.5 and earlier allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PDF file, related to (1) glib/poppler-page.cc; (2) ArthurOutputDev.cc, (3) CairoOutputDev.cc, (4) GfxState.cc, (5) JBIG2Stream.cc, (6) PSOutputDev.cc, and (7) SplashOutputDev.cc in poppler/; and (8) SplashBitmap.cc, (9) Splash.cc, and (10) SplashFTFont.cc in splash/. NOTE: this may overlap CVE-2009-0791.	2009-11-02	10.0	CVE-2009-3605 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM UBUNTU SECUNIA CONFIRM CONFIRM CONFIRM
	Stack-based buffer overflow in SafeNet SoftRemote			CVE-2009-2961

safenet-inc -- softremote	10.8.5 (Build 2) and 10.3.5 (Build 6), and possibly other versions before 10.8.9, allows local users to execute arbitrary code via a long string in a (1) TREENAME or (2) GROUPNAME Policy file (spd).	2009-11-04	7.2	3001 VUPEN MISC SECTRACK BUGTRAQ
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the Solaris Trusted Extensions Policy configuration in Sun Solaris 10, and OpenSolaris snv_37 through snv_125, might allow remote attackers to execute arbitrary code by leveraging access to the X server.	2009-11-02	7.5	CVE-2009-3839 SUNALERT
sun -- solaris	Trusted Extensions in Sun Solaris 10 interferes with the operation of the xscreensaver-demo command for the XScreenSaver application, which makes it easier for physically proximate attackers to access an unattended workstation for which the intended screen locking did not occur, related to the "restart daemon."	2009-11-03	7.2	CVE-2009-3851 CONFIRM
sun -- jdk sun -- jre	The Java Update functionality in Java Runtime Environment (JRE) in Sun Java SE in JDK and JRE 5.0 before Update 22 and JDK and JRE 6 before Update 17, when a non-English version of Windows is used, does not retrieve available new JRE versions, which allows remote attackers to leverage vulnerabilities in older releases of this software, aka Bug Id 6869694.	2009-11-05	7.5	CVE-2009-3864 VUPEN SUNALERT
sun -- jdk sun -- jre	The launch method in the Deployment Toolkit plugin in Java Runtime Environment (JRE) in Sun Java SE in JDK and JRE 6 before Update 17 allows remote attackers to execute arbitrary commands via a crafted web page, aka Bug Id 6869752.	2009-11-05	9.3	CVE-2009-3865 VUPEN BID SUNALERT
sun -- jdk sun -- jre	The Java Web Start Installer in Sun Java SE in JDK and JRE 6 before Update 17 does not properly use security model permissions when removing installer extensions, which allows remote attackers to execute arbitrary code by modifying a certain JNLP file to have a URL field that points to an unintended trusted application, aka Bug Id 6872824.	2009-11-05	9.3	CVE-2009-3866 MISC SUNALERT
sun -- jdk sun -- jre sun -- sdk	Stack-based buffer overflow in the HsbParser.getSoundBank function in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to execute arbitrary code via a long file: URL in an argument, aka Bug Id 6854303.	2009-11-05	9.3	CVE-2009-3867 MISC SUNALERT
sun -- jdk sun -- jre sun -- sdk	Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 does not properly parse color profiles, which allows remote attackers to gain privileges via a crafted image file, aka Bug Id 6862970.	2009-11-05	9.3	CVE-2009-3868 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Stack-based buffer overflow in the setDiffICM function in the Abstract Window Toolkit (AWT) in Java Runtime Environment (JRE) in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to execute arbitrary code via a crafted argument, aka Bug Id 6872357.	2009-11-05	9.3	CVE-2009-3869 MISC SUNALERT

sun -- jdk sun -- jre sun -- sdk	Heap-based buffer overflow in the setBytePixels function in the Abstract Window Toolkit (AWT) in Java Runtime Environment (JRE) in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to execute arbitrary code via crafted arguments, aka Bug Id 6872358.	2009-11-05	9.3	CVE-2009-3871 MISC SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in the JPEG JFIF Decoder in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to gain privileges via a crafted image file, aka Bug Id 6862969.	2009-11-05	10.0	CVE-2009-3872 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Integer overflow in the JPEGImageReader implementation in the ImageI/O component in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to execute arbitrary code via large subsample dimensions in a JPEG file that triggers a heap-based buffer overflow, aka Bug Id 6874643.	2009-11-05	9.3	CVE-2009-3874 MISC SUNALERT
sun -- java_system_web_server	Buffer overflow in Sun Java System Web Server 7.0 Update 6 has unspecified impact and remote attack vectors, as demonstrated by the vd_sjws module in VulnDisco Pack Professional 8.12. NOTE: as of 20091105, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-11-05	9.3	CVE-2009-3878 XF VUPEN OSVDB MISC MISC SECUNIA MISC
symantec -- altiris_deployment_solution symantec -- altiris_management_platform symantec -- altiris_notification_server	Stack-based buffer overflow in the BrowseAndSaveFile method in the Altiris eXpress NS ConsoleUtilities ActiveX control 6.0.0.1846 in AeXNSConsoleUtilities.dll in Symantec Altiris Notification Server (NS) 6.0 before R12, Deployment Server 6.8 and 6.9 in Symantec Altiris Deployment Solution 6.9 SP3, and Symantec Management Platform (SMP) 7.0 before SP3 allows remote attackers to execute arbitrary code via a long string in the second argument.	2009-11-03	9.3	CVE-2009-3031 CONFIRM
typo3 -- typo3	The Backend subcomponent in TYPO3 4.0.13 and earlier, 4.1.x before 4.1.13, 4.2.x before 4.2.10, and 4.3.x before 4.3beta2, when the DAM extension or ftp upload is enabled, allows remote authenticated users to execute arbitrary commands via shell metacharacters in a filename.	2009-11-02	8.5	CVE-2009-3631 VUPEN BID
typo3 -- typo3	The Install Tool subcomponent in TYPO3 4.0.13 and earlier, 4.1.x before 4.1.13, 4.2.x before 4.2.10, and 4.3.x before 4.3beta2 allows remote attackers to gain access by using only the password's md5 hash as a credential.	2009-11-02	7.5	CVE-2009-3635 BID

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
---------------------------	-------------	-----------	------------	---------------------

arubanetworks -- arubaos	ArubaOS 3.3.1.x, 3.3.2.x, RN 3.1.x, 3.4.x, and 3.3.2.x-FIPS on the Aruba Mobility Controller allows remote attackers to cause a denial of service (Access Point crash) via a malformed 802.11 Association Request management frame.	2009-11-02	5.0	CVE-2009-3836 VUPEN BID CONFIRM SECUNIA
ecouriersoftware -- e-courirer_cms	Multiple cross-site scripting (XSS) vulnerabilities in e-Courier CMS allow remote attackers to inject arbitrary web script or HTML via the UserGUID parameter to home/index.asp and other unspecified vectors.	2009-11-06	4.3	CVE-2009-3901 SECUNIA MISC
ecouriersoftware -- e-courirer_cms	Multiple cross-site scripting (XSS) vulnerabilities in e-Courier CMS allow remote attackers to inject arbitrary web script or HTML via the UserGUID parameter to (1) Wizard_tracking.asp, (2) wizard_oe2.asp, (3) your-register.asp, (4) main-whyregister.asp, and (5) your.asp in home/, and other unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-11-06	4.3	CVE-2009-3905 SECUNIA
gejosoft -- gejosoft	Cross-site scripting (XSS) vulnerability in GejoSoft allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to the default URI in photos/tags.	2009-11-04	4.3	CVE-2009-3858 XF VUPEN SECUNIA MISC OSVDB
idefense -- comraider	Multiple insecure method vulnerabilities in Idefense Labs COMRaider allow remote attackers to create or overwrite arbitrary files via the (1) CreateFolder and (2) Copy methods. NOTE: this might only be a vulnerability in certain insecure configurations of Internet Explorer.	2009-11-04	5.8	CVE-2009-3860 BID BUGTRAQ MISC
james_clark -- expat	The updatePosition function in lib/xmltok_impl.c in libexpat in Expat 2.0.1, as used in Python, PyXML, w3c-libwww, and other software, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with crafted UTF-8 sequences that trigger a buffer over-read, a different vulnerability than CVE-2009-2625.	2009-11-03	5.0	CVE-2009-3720 CONFIRM MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MANDRIVA CONFIRM MISC MLIST CONFIRM CONFIRM
linux -- kernel linux -- kernel	The get_instantiation_keyring function in security/keys/keyctl.c in the KEYS subsystem in the Linux kernel before 2.6.32-rc5 does not properly maintain the reference count of a keyring, which allows local users to gain privileges or cause a denial of service (OOPS) via vectors involving calls to this function without specifying a keyring by ID, as demonstrated by a series of keyctl request2 and keyctl list commands.	2009-11-02	4.6	CVE-2009-3624 CONFIRM MISC SECUNIA MLIST MLIST CONFIRM

linux -- kernel linux -- kernel	Multiple race conditions in fs/pipe.c in the Linux kernel before 2.6.32-rc6 allow local users to cause a denial of service (NULL pointer dereference and system crash) or gain privileges by attempting to open an anonymous pipe via a /proc/*/fd/ pathname.	2009-11-04	6.9	CVE-2009-3547 REDHAT REDHAT REDHAT REDHAT CONFIRM BID CONFIRM MLIST MLIST MLIST CONFIRM
mahara -- mahara	Mahara before 1.0.13, and 1.1.x before 1.1.7, allows remote authenticated institution administrators to reset a site administrator password via unspecified vectors.	2009-11-03	6.5	CVE-2009-3298 VUPEN BID CONFIRM
mahara -- mahara	Cross-site scripting (XSS) vulnerability in the resume blocktype in Mahara before 1.0.13, and 1.1.x before 1.1.7, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-11-03	4.3	CVE-2009-3299 VUPEN BID CONFIRM
novell -- edirectory	The NDSD process in Novell eDirectory 8.7.3 before 8.7.3.10 ftf2 and eDirectory 8.8 before 8.8.5 ftf1 does not properly handle certain LDAP search requests, which allows remote attackers to cause a denial of service (application hang) via a search request with a NULL BaseDN value.	2009-11-04	5.0	CVE-2009-3862 CONFIRM
novell -- groupwise	Buffer overflow in the gxmim1.dll ActiveX control in Novell Groupwise Client 7.0.0.1294 allows remote attackers to cause a denial of service (application crash) via a long argument to the SetFontFace method.	2009-11-04	5.0	CVE-2009-3863 MILWORM
softonic -- scite	Buffer overflow in Softonic International SciTE 1.72 allows user-assisted remote attackers to cause a denial of service (application crash) via a Ruby (.rb) file containing a long string, which triggers the crash when a scroll bar is used.	2009-11-04	4.3	CVE-2009-3857 XF MILWORM
sun -- jdk sun -- jre sun -- sdk	The MessageDigest.isEqual function in Java Runtime Environment (JRE) in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to spoof HMAC-based digital signatures, and possibly bypass authentication, via unspecified vectors related to "timing attack vulnerabilities," aka Bug Id 6863503.	2009-11-05	5.0	CVE-2009-3875 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to cause a denial of service (memory consumption) via crafted DER encoded data, which is not properly decoded by the ASN.1 DER input stream parser, aka Bug Id 6864911.	2009-11-05	5.0	CVE-2009-3876 SUNALERT
sun -- jdk sun -- jre sun -- sdk	Unspecified vulnerability in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to cause a denial of service (memory consumption) via crafted HTTP headers, which are not properly parsed by the ASN.1 DER input	2009-11-05	5.0	CVE-2009-3877 SUNALERT

	stream parser, aka Bug Id 6864911.			
twilightcms -- twilight_cms	Cross-site scripting (XSS) vulnerability in the default URI in news/ in Twilight CMS before 4.1 allows remote attackers to inject arbitrary web script or HTML via the calendar parameter. NOTE: some of these details are obtained from third party information.	2009-11-04	4.3	CVE-2009-3856 SECUNIA MISC
typo3 -- typo3	The Backend subcomponent in TYPO3 4.0.13 and earlier, 4.1.x before 4.1.13, 4.2.x before 4.2.10, and 4.3.x before 4.3beta2 allows remote authenticated users to determine an encryption key via crafted input to a tt_content form element.	2009-11-02	4.0	CVE-2009-3628 BID
typo3 -- typo3	The Backend subcomponent in TYPO3 4.0.13 and earlier, 4.1.x before 4.1.13, 4.2.x before 4.2.10, and 4.3.x before 4.3beta2 allows remote authenticated users to place arbitrary web sites in TYPO3 backend framesets via crafted parameters, related to a "frame hijacking" issue.	2009-11-02	4.0	CVE-2009-3630 VUPEN BID
typo3 -- typo3	SQL injection vulnerability in the traditional frontend editing feature in the Frontend Editing subcomponent in TYPO3 4.0.13 and earlier, 4.1.x before 4.1.13, 4.2.x before 4.2.10, and 4.3.x before 4.3beta2 allows remote authenticated users to execute arbitrary SQL commands via unspecified parameters.	2009-11-02	6.5	CVE-2009-3632 XF VUPEN BID CONFIRM SECUNIA MLIST
typo3 -- typo3	Cross-site scripting (XSS) vulnerability in the t3lib_div::quoteJSvalue API function in TYPO3 4.0.13 and earlier, 4.1.x before 4.1.13, 4.2.x before 4.2.10, and 4.3.x before 4.3beta2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to the sanitizing algorithm.	2009-11-02	4.3	CVE-2009-3633 VUPEN BID
typo3 -- typo3	Cross-site scripting (XSS) vulnerability in the Install Tool subcomponent in TYPO3 4.0.13 and earlier, 4.1.x before 4.1.13, 4.2.x before 4.2.10, and 4.3.x before 4.3beta2 allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2009-11-02	4.3	CVE-2009-3636 VUPEN BID
vmware -- ace vmware -- esx vmware -- esxi vmware -- fusion vmware -- player vmware -- server vmware -- workstation	VMware Workstation 6.5.x before 6.5.3 build 185404, VMware Player 2.5.x before 2.5.3 build 185404, VMware ACE 2.5.x before 2.5.3 build 185404, VMware Server 1.x before 1.0.10 build 203137 and 2.x before 2.0.2 build 203138, VMware Fusion 2.x before 2.0.6 build 196839, VMware ESXi 3.5 and 4.0, and VMware ESX 2.5.5, 3.0.3, 3.5, and 4.0, when Virtual-8086 mode is used, do not properly set the exception code upon a page fault (aka #PF) exception, which allows guest OS users to gain privileges on the guest OS by specifying a crafted value for the cs register.	2009-11-02	6.9	CVE-2009-2267 CONFIRM
vmware -- esx vmware -- esxi vmware -- server	Directory traversal vulnerability in VMware Server 1.x before 1.0.10 build 203137 and 2.x before 2.0.2 build 203138 on Linux, VMware ESXi 3.5, and VMware ESX 3.0.3 and 3.5 allows remote attackers to read arbitrary files via unspecified vectors.	2009-11-02	4.3	CVE-2009-3733 VUPEN CONFIRM BID BUGTRAQ SECTRACK SECTRACK SECUNIA MLIST

[Back to top](#)

Low Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sun -- jdk sun -- jre sun -- sdk	The JPEG Image Writer in Sun Java SE in JDK and JRE 5.0 before Update 22, JDK and JRE 6 before Update 17, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to gain privileges via a crafted image file, related to a "quantization problem," aka Bug Id 6862968.	2009-11-05	0.0	CVE-2009-3873 SUNALERT
typo3 -- typo3	Multiple cross-site scripting (XSS) vulnerabilities in the Backend subcomponent in TYPO3 4.0.13 and earlier, 4.1.x before 4.1.13, 4.2.x before 4.2.10, and 4.3.x before 4.3beta2 allow remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2009-11-02	3.5	CVE-2009-3629 XF VUPEN BID CONFIRM SECUNIA MLIST MLIST
Back to top				

Last updated November 09, 2009

 Print This Document